PLATTFORM INDUSTRIE 4.0

ERGEBNISPAPIER

Technischer Überblick: Sichere Identitäten

Impressum

Herausgeber
Bundesministerium für Wirtschaft
und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Redaktionelle Verantwortung
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

Gestaltung und Produktion
PRpetuum GmbH, München

Stand
April 2016

Druck
Spreedruck Berlin GmbH

Bildnachweis
Maxsim – Fotolia (Titel); Petrovich12 – Fotolia (S. 8);
kebox – Fotolia (S. 10); tatomm – Fotolia (S. 14);
Sergey Nivens – Fotolia (S. 17)

Das Bundesministerium für Wirtschaft und Energie ist mit dem audit berufundfamilie® für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie gGmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.

Diese und weitere Broschüren erhalten Sie bei:
Bundesministerium für Wirtschaft und Energie
Referat Öffentlichkeitsarbeit
E-Mail: publikationen@bundesregierung.de
www.bmwi.de

Zentraler Bestellservice:
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhalt

Tabellenverzeichnis

Abbildungsverzeichnis

1. Einleitung

Ziel des Papiers ist es, eine gemeinsame Übersicht hinsichtlich der Security-Herausforderungen, Anforderungen und Ansätze für sichere Identitäten in Industrie 4.0-Umgebungen zu formulieren. Das Dokument stellt den für Industrie 4.0 zusätzlichen Handlungsbedarf für den Einsatz von hinreichend sicheren Identitätsmerkmalen dar.

Die Inhalte werden auf einer generischen Ebene zur Sicherstellung einer guten Übertragbarkeit skizziert. Dies trägt der Situation Rechnung, dass jede detaillierte Security-Betrachtung eine Einzelfallbetrachtung sein muss, um die ausschlaggebenden Rahmenbedingungen berücksichtigen zu können. Entsprechend wird von einer konkreten Projekt- oder Implementierungsbeschreibung abgesehen.

Das Dokument richtet sich an Entscheider und Anwender im Industrie 4.0-Kontext. Für diese Zielgruppe werden die zu beachtenden Rahmenbedingungen – „was gilt als sichere Identität?“ –, die Leitprinzipien und die gewonnenen Erkenntnisse zur Security exemplarisch dargestellt.

Warum „sichere Identitäten“?

In dem Ergebnisbericht der Plattform Industrie 4.0 „Umsetzungsstrategie Industrie 4.0“ (April 2015) wurde bereits dargestellt, dass ein sicherer Informationsaustausch entlang des gesamten Wertschöpfungsprozesses für Industrie 4.0 essentiell ist. Dies erfordert die eindeutige Identifikation und Authentifizierung von Menschen, Maschinen und Prozessen sowie den Nachweis bestimmter Eigenschaften. Dabei wurde ebenfalls die Notwendigkeit der Suche nach Möglichkeiten zur Abstufung der Sicherheit festgestellt.[1]

Sichere Identitäten sind der Ausgangspunkt für die Sicherheitskette, welche die Datenerhebung, den -transport und die -verarbeitung auf Hardware-, Software- und Prozessebene absichert. Sie fungieren als Voraussetzung für viele weitere Schutzmaßnahmen. Wenn es einem Angreifer gelingt, unberechtigt eine Identität anzunehmen, laufen alle darauf aufbauenden Maßnahmen wie z. B. der Zugriffsschutz ins Leere. Hauptziel von sicheren Identitäten ist der Start der Vertrauenskette in der automatisierten Kommunikation. Sichere Identitäten unterstützen die bekannten Schutzziele:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Im täglichen Leben ist dies mit einer Eingangskontrolle durch einen Pförtner zu vergleichen. Dieser kontrolliert z. B. anhand eines Firmenausweises die Berechtigung zum Zugang. Dabei wird die Echtheit und Gültigkeit des Firmenausweises geprüft sowie ein Abgleich mit einer Sperrliste durchgeführt. Anschließend verifiziert er die Zuordnung zwischen Ausweis und Inhaber des Papiers mit den hinterlegten Informationen (Passbild, Größe, Augenfarbe, ggf. biometrische Merkmale). Ähnlich muss auch in der digitalen Welt geprüft werden, wer Zugriff auf Daten erhält bzw. einen Auftrag erteilt und ob derjenige dazu berechtigt ist. In beiden Welten sind dies elementare Vorgänge, die mit entsprechender Sorgfalt betrieben werden müssen und die Basis für erfolgreiches Handeln darstellen.

Sichere Identitäten sind auch für rechtliche und kaufmännische Prozesse von Relevanz. Grundsätzlich erhöhen sie die Transparenz von Abläufen. Dadurch wird leichter nachvollziehbar, wer, wie, wann und mit welchen Rechten kommuniziert und ggf. entscheidet. Verallgemeinernd lässt sich sagen: Je verlässlicher, vertrauenswürdiger und nachvollziehbarer Identitäten sind, desto eher ist die Übertragung von (automatisierten) Ausführungs- und Entscheidungskompetenzen für Menschen, Maschinen und Komponenten denkbar. Sichere Identitäten können somit ein Enabler für Effizienzgewinne sein.

Ausgangslage für sichere Identitäten in der Industrie 3.0

Bei der Industrie 3.0 existieren vorrangig die in der nachfolgenden Abbildung illustrierten Interaktionen:

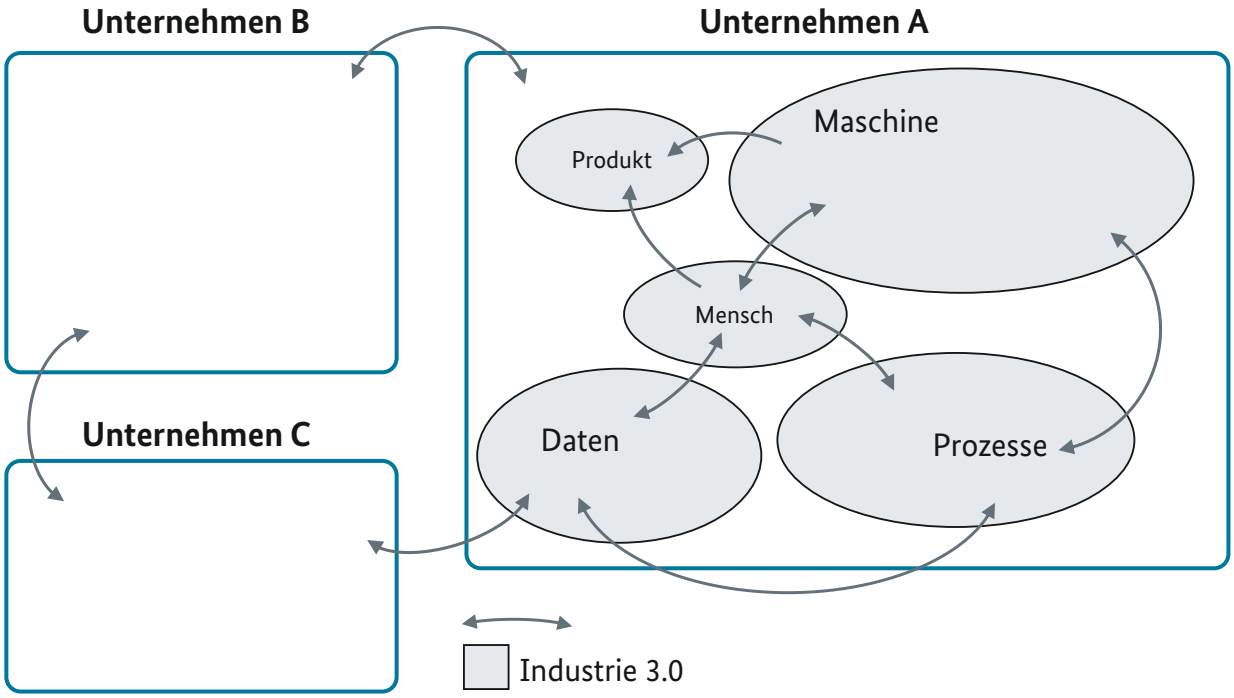
- Innerhalb einer Organisation interagieren Menschen, Daten, Prozesse und Maschinen. Das Produkt nimmt nur passiv hieran teil: Es wird erzeugt.

- Organisationen interagieren untereinander über traditionelle und definierte Wege, bei denen selten direkt Daten, Prozesse und Maschinen über Organisationsgrenzen hinweg interagieren. Vielmehr existiert zwischen den Organisationen ein Perimeterschutz, der diese direkte Interaktion bewusst erschwert oder verhindert.

In der Industrie 3.0 sind Menschen, Maschinen, Prozesse und Unternehmen allen bekannt und es existieren feste Verbindungen und Zuordnungen.

1 vgl. „Abschlussbericht 2015“, S. 53 ff.

Abbildung 1: Kommunikations- und Vertrauensbeziehungen bei Industrie 3.0



Quelle: Plattform Industrie 4.0

Der Fokus der Sicherheitsbetrachtung im Automatisierungsumfeld liegt heute bei der Absicherung des unternehmensinternen Netzwerkes nach außen.

Insgesamt sind derzeit sichere Identitäten meist nicht im System integriert, sondern werden als Add-on durch spezielle Security-Produkte nachgeliefert (Dongle, HW-Token, SW-Token). Eine ganzheitliche Abstimmung der Zuständigkeiten zwischen dem Office-Bereich – oft auch als Information Technology (IT) bezeichnet – und der Produktionsebene – auch als Operations Technology (OT) bezeichnet – gibt es häufig noch nicht flächendenkend, um Erfahrungen in geeigneter Art und Weise auszutauschen. Gleiches gilt für Security-by-Design in den Produkten und Maschinen.

Sichere Identitäten werden derzeit vor allem auf Anwenderebene eingesetzt, z. B. für den Zugang zur Fernwartung, für Lizenzierungsmechanismen oder im Office-Bereich für die Verschlüsselung von E-Mails. Zusätzlich wird der Nachbauschutz für Hard- und Software-Komponenten oftmals durch Einsatz kryptografisch basierter Identifikationsmechanismen unterstützt (z. B. Authentifikations-Chips).

Es existiert keine etablierte Sicherheitsinfrastruktur zur Unterstützung von sicheren Identitäten über Unternehmensgrenzen (Sicherheitsdomänen) hinweg.

Ein hoher Nachholbedarf an Security allgemein und speziell hinsichtlich sicherer Identitäten besteht bei kleinen und mittleren Unternehmen. Geringe Methodenkompetenz in der Einschätzung und Bewertung der Sicherheitsrisiken sowie fehlende Standards und allgemein anerkannte Leitlinien verhindern vielfach die Umsetzung konkreter Maßnahmen.

Insgesamt fehlt es oft schon an einer funktionsfähigen Infrastruktur im Unternehmen und den organisatorischen Prozessen wie einer Public-Key-Infrastruktur (PKI), um das erforderliche Sicherheitsmanagement für sichere Identitäten abzubilden.

Wie sieht die Situation bei Industrie 4.0 aus?

Im Unterschied dazu entsteht bei Industrie 4.0 durch die Bildung von Wertschöpfungsnetzwerken und zunehmende Flexibilisierung eine viel höhere Interaktionsdichte zwischen Teilen eines Unternehmens und von Teilen verschiedener Unternehmen über deren Grenzen hinweg.

Zu den bisher interagierenden Menschen, Software-Prozessen und Maschinen kommen Interaktionen mit den folgenden Akteuren hinzu:

- Austauschbare und daher am Anfang unbekannte Maschinenkomponenten
- Digitale Abbilder (Verwaltungsschalen[2]) von Maschinen, Komponenten und Produkten

Insbesondere hinsichtlich der Flexibilisierung der eigenen Unternehmensabläufe sind Identitäten – allein schon aus rechtlichen Gründen – die notwendige Ausgangsbasis fast aller Geschäftsprozesse und die Flexibilisierung wäre ohne sie in der Industrie 4.0 de facto nicht zu leisten. Was bereits für die Industrie 3.0 gilt, wird für Industrie 4.0 zum unverzichtbaren Grundsatz: Nur wer sich vertraut (Menschen und Maschinen), sollte miteinander kommunizieren. Identitäten besitzen daher eine zentrale Bedeutung für den Gesamtprozess.

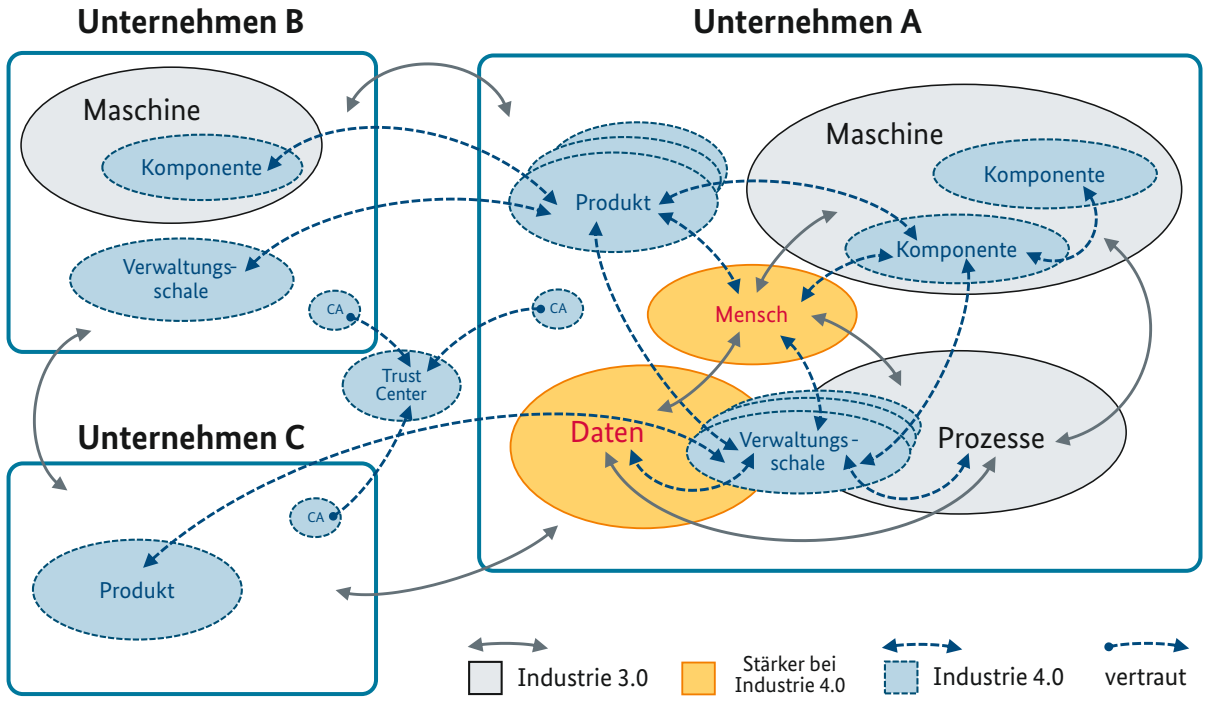
Industrie 4.0 sieht auch vor, rechtlich relevante Kommunikation abzubilden, zum Beispiel im Rahmen von Bestell- und Logistikprozessen. Daher sind bei der Betrachtung die weiteren Schutzziele

- Authentizität
- Verbindlichkeit/Nichtabstreitbarkeit
- Zurechenbarkeit

zu berücksichtigen.

Geschäftsbeziehungen werden also auf rein elektronischer Basis abgeschlossen und Maschinen kommunizieren immer stärker direkt miteinander. Dies erfordert, dass bisher übliche Prüfungen aus der physikalischen Welt in die elektro-

Abbildung 2: Kommunikations- und Vertrauensbeziehungen bei Industrie 4.0



Quelle: Plattform Industrie 4.0

2 siehe Fußnote 1 Seite 4

nische übertragen werden müssen. So gilt es beispielsweise bei Vertragsverhandlungen neben der sicheren Identifizierung auch weitere Informationen wie z. B. Bonität zu erhalten. Ähnliches gilt für die Kommunikation zwischen Maschinen oder Komponenten. Auch hier muss sichergestellt sein, dass ein Zugriff nur bei berechtigtem Interesse erfolgt, Informationen von einem bestimmten Sensor kommen oder Daten nur an bestimmte Maschinen übertragen werden.

Gängige Verwendung von Identitäten

Für Hersteller, Integratoren und Betreiber sind Identitäten beispielsweise zur

- Prüfung & Bestätigung der Systemintegrität von Komponenten oder Maschinen,
- Steuerbarkeit von Prozessen, Zugriffen und Berechtigungen über Zeit, Ort oder Domäne,
- Echtheitsprüfung von Komponenten oder Ersatzteilen,
- Durchführung von Fernwartungen bzw. vorbeugende Wartung (Predictive Maintenance),
- Qualitätssicherung im Produktionsprozess (z. B. Prozessverriegelung),
- Inventarisierung von Produkten,
- Erfüllung von Compliance- und Dokumentationsvorschriften und
- Erfüllung von Herkunftsnachweisanforderungen

notwendig.

Beispielhafte Verwendung finden Identitäten in den Anwendungsszenarien der Plattform Industrie 4.0[3]:

- M2M-Vertragaushandlung oder Zuordnung von Selbstbeschreibungen (Szenario 1)
- Rückverfolgung (Traceability) von ausgelieferten Komponenten und Ersatzteilen oder Freischaltung von Features (Komponente und Feature müssen identifizierbar sein) (Szenario 4)
- Identifikation von Fertigungsmodulen, deren Funktionalität und Kompatibilität mit anderen Modulen (Szenario 5)

Anhand dieser Beispiele wird deutlich, dass Identitäten sehr weit verbreitet sind und unterschiedliche Ziele verfolgen. Die Spanne reicht dabei von einer Typkennzeichnung bis hin zu Identitäten, mit denen geschäftswirksame Handlungen verbunden sind. Im einen Fall reicht eine einfache Typkennzeichnung beispielsweise in Form eines Barcodes. In dem anderen Szenario ist eine sichere und manipulationsgeschützte Identität notwendig. Eine Übersicht über Identitäten ist aus Tabelle 1 ersichtlich.

Welche Objekte welche Art von Identität benötigen, muss im Rahmen einer Sicherheitsbetrachtung und Risikoanalyse festgestellt werden. Das Dokument liefert Informationen zu unterschiedlichen Arten von Identitäten und den Anforderungen. Es gibt Hinweise, die helfen sollen, zu entscheiden, ob eine Identität für den gewählten Einsatzzweck sicher, vertrauenswürdig und geeignet ist.

3 Plattform Industrie 4.0: „Abbildung der Anwendungsszenarien auf die Forschungsroadmap“

2. Kurze Begriffserläuterung

Im Folgenden werden einige grundlegende Begriffe des Identitätsmanagements, wie sie in diesem Dokument genutzt werden, definiert (angelehnt an [ISO24760-1] und [BSI TR 3107-1], Abschnitt 2.1 und 2.2):

- Eine Entität ist konkretes oder abstraktes Objekt einschließlich Assoziationen zwischen Objekten [DIN 4002-4:2013-09].
  - **Hinweis 1:** Konkrete Objekte können eine Person, eine Maschine, ein Produkt oder eine Organisation (Unternehmen/Vertragspartner) sein.
  - **Hinweis 2:** Abstrakte Objekte könnten digitale Datensätze, Dateien oder Patente sein.
- Ein Attribut oder ein Datum ist eine Charakteristik oder eine Eigenschaft einer Entität.
  - **Hinweis:** Beispiele für Attribute oder Daten einer Person sind Name oder Geburtsdatum. Attribute von Maschinen umfassen etwa Bezeichnung der Maschine oder deren Funktionen. Beispiele für Produkte können Herstellungsdatum, Artikelnummer, Gewicht, Farbe etc. sein.
- Eine Identität (ID) ist eine Eigenschaft einer Entität, gekennzeichnet durch eine Menge von Attributen. Eine Entität kann mehrere Identitäten haben, ebenso können mehrere Entitäten die gleiche Identität haben.
  - **Hinweis:** Vergleichbar ist der Anwendungsfall mit einer Hausanschrift. Das Gebäude besitzt eine klare Identität, die für mehrere Hausbewohner gilt. Beschränkt auf die Hausnummer besitzen die Hausbewohner keine eindeutige Identität. Eine Identität ist daher im Allgemeinen nicht eindeutig, kann dies aber in einem bestimmten Anwendungskontext sein.
- Eine eindeutige Identität (UID) ist die spezifizierte Menge an Attributen, die innerhalb eines bestimmten Anwendungskontextes die zugehörige Entität eindeutig repräsentiert.
  - **Hinweis:** Eindeutige Identitäten sind genau einer Entität oder Entitätsklasse zugeordnet, eine Entität wiederum kann mehrere eindeutige Identitäten besitzen, z. B. durch Eigentumsübergang in verschiedenen Unternehmen.

- Eine Sichere Identität (SID) ist eine eindeutige Identität mit zusätzlichen Sicherheitseigenschaften für eine belastbar vertrauenswürdige Authentifizierung der Entität (d. h. mit angemessenen Maßnahmen zur Verhinderung der Vortäuschung einer falschen Identität).
    - **Hinweis:** Dabei ist die Erfüllung der Sicherheitsanforderungen für ein Zielsystem technisch auf verschiedene Arten möglich (siehe Beispiele in der Tabelle 1). Um hohe Sicherheitsanforderungen erfüllen zu können, empfiehlt es sich, die Identitätsinformation mit einer physikalischen Eigenschaft, also einem zweiten Faktor, zu verbinden. Diese Eigenschaft muss so beschaffen sein, dass sie nicht, oder nur durch (für einen Angreifer) unverhältnismäßig hohen Aufwand, kopiert oder gezielt verändert werden kann.
    - **Hinweis:** Für IT-gebundene Systeme kann ein hohes Sicherheitsniveau mittels HW-basierten kryptografischen Authentifikationsfunktionen realisiert werden. Die Identitätsinformation wird dabei über ein kryptographisches Zertifikat an einen geschützt gespeicherten, geheimen Schlüssel gekoppelt, dessen lokale Anwendung dann als Beweis der Identität verwendet wird.
- **Authentizität:** Eigenschaft eines Attributs. Ein Attribut ist dann authentisch, wenn es mit einer Behauptung tatsächlich übereinstimmt; wenn also die tatsächliche Eigenschaft der behaupteten Eigenschaft entspricht.
    - **Hinweis:** Eine versendete Nachricht wird z. B. als authentisch bzgl. der Herkunft bezeichnet, wenn der tatsächliche Absender mit dem in den Metadaten (z. B. Absenderadresse) angegebenen Absender identisch ist.
- **Authentifikation:** Feststellung der Authentizität. Eingangsgrößen: Attribut eines Absenders und empfangene Mitteilung oder Attribute eines Zugreifenden und Zugriffsgesuch. Ausgangsgröße: ist authentisch [ja/nein].
    - **Beispiel:** Eine typische M2M-Authentifikation besteht aus geeigneten Maßnahmen wie z. B. Challenge-Response-Verfahren oder PKI-basierter Authentifizierung mittels etablierter kryptografischer Funktionen. Der Absender oder Zugreifende belegt dabei seine Authentizität durch erfolgreiche Durchführung der eingesetzten kryptografischen Verfahren und damit durch Kenntnis des/der notwendigen kryptografischen Schlüssel.
- **Vertrauen:** Explizit geprüfte und bestätigte Eignung der eingesetzten Security-Maßnahmen zur Erfüllung der Security-Anforderungen. Es werden Überprüfungen/Audits/Evaluationen eingesetzt, die zusammen ein Vertrauensniveau schaffen. Eine Security-Richtlinie legt fest, welches Vertrauensniveau als ausreichend erachtet wird. Derart erfolgreich geprüfte Security-Maßnahmen gelten dann im Wirkbereich der Richtlinie als vertrauenswürdig hinsichtlich der Erbringung ihrer Security-Schutzfunktion. Die Richtlinie wird bei Bedarf aktualisiert und enthält auch zeitliche Anforderungen wie z. B. zulässige Gültigkeitsdauer zwischen zwei Überprüfungen, siehe dazu die ausführliche Beschreibung im Anhang A3.
- **Identitätsträger:** Z. B. physisches Objekt (RFID- oder QR-Code-Aufkleber) oder elektronisches Bauteil (TPM-Modul), das die Identität der Entität bereitstellt; siehe dazu die Tabelle 3.

3. Identitätstypen

Tabelle 1 klassifiziert den Begriff „Identitäten“ beispielhaft in die drei Typen „Identität (ID)“, „Eindeutige Identität (UID)“ und „Sichere Identität (SID)“. Diese Typisierung unterscheidet Identitäten nach den Anforderungen an die Sicherheit, die im Zielsystem zu erfüllen sind, eine feinere Granulierung der SID wird in Anhang 2 herausgearbeitet

Eigenschaften der Identitäten

Im Folgenden soll auf die grundsätzlichen Merkmale von Identitäten eingegangen werden:

- **Grad der Eindeutigkeit der Identität (einfach, eindeutig, sicher)**
- **Inhaber der Identität: Mensch, Maschine oder Produkt etc.**
- **Bindung des Identitätsträger an den Inhaber**
  - Zeitlich (einmalig vs. wiederverwendbar)
  - Robustheit der Bindung
- **Einschränkung der Gültigkeit** der Identität:
  - Raum: Werksgelände vs. global
  - Zeit: Stunde vs. dauerhaft

Grundlegend ist die Frage nach der Notwendigkeit eines bestimmten Identitätstyps vor dem Hintergrund der jeweiligen Schutzziele. Wenn beispielsweise Produkte mit einer einfachen Identität versehen werden, so kann dies ausreichend sein, um sicherzustellen, dass nur diese Produktklasse verwendet wird. In diesem Fall haben mehrere Entitäten die gleiche Identität. In anderen Fällen möchte ein Unternehmen eindeutig bestimmen, welche Maschine eine Tätigkeit zu welchem Zeitpunkt ausgeführt hat. Dies erfordert eine eindeutige Identität. Ist hingegen der Schutz vor Fälschung, Diebstahl und/oder Missbrauch gefordert, sollte eine sichere Identität gewählt werden.

Auch der Faktor Zeit hat Einfluss auf Identitäten. So können sich Identitätsattribute ändern. Der Wechsel eines Menschen von einem Unternehmen zu einem anderen Unternehmen hat eine in den meisten Fällen neue Identität zur Folge. (Dies wird im Abschnitt zum Lebenszyklus noch ausführlicher betrachtet.) So kann es auch in der Fertigung notwendig sein, dass mit einer Identität nur zeitlich befris-

Tabelle 1: Typen von Identitäten nach Security-Merkmalen mit Technologiebeispielen

		Identität (ID)	Eindeutige Identität (UID)	Sichere Identität (SID)
Security-Merkmale	**Tiefe der Identifikation; Anspruch/Ziel**	Identifikation von Artikeln, Herstellern oder Personen (Klassen von Entitäten)	Identifikation von individuellen Entitäten	Identifikation und Authentifikation von individuellen Entitäten
	Identifikation	X[1]	X	X
	Unterscheidung innerhalb einer Klasse	–	X	X
	Integrität	–	X	X
	Fälschungsresistenz	–	(X)	X
	Offline-Identifikation	X	(X)	(X)
	Authentifikation	–	–[2]	X
	Offline-Authentifikation	–	–	(X)
Beispiele aktueller Technologien	**Digitale ID**	Mit Public Key signierte Software	IP-Adresse, MAC[3]-Adresse, GUID	TPM[4] – (mit enthaltenem Sicherheitsanker oder Zertifikat)
	RFID[5]	RFID-Tag mit gespeicherter Klasseninformation (z. B. Artikelnummer)	RFID-Tag mit gespeicherter, fester UID	Sicherer Mikroprozessor (verschiedene Lösungen)
	DMC (data matrix code)	DMC mit GTIN[6]	DMC mit SGTIN	– (nur mit zweitem Faktor möglich)
	QR-Code	QR-Code	QR-Code mit Seriennummer	– (nur mit zweitem Faktor möglich)
	Mustererkennung (grafisch)	Visual Recognition (Umrisse, Abmaße)	zusätzliche Faktoren (z. B. Zeit und Andruck bei Unterschrift)	–
	Mautvignette	Vignette	Vignette mit Seriennummer	Mautsystem – OBU (on board unit)
	OVD (Optical Variable Devices)	Hologramm, Sicherheitsfarbe, Sicherheitsmaterial oder ähnlich	Hologramm oder Sicherheitsdruck mit Seriennummer	– (nur mit zweitem Faktor möglich)
	Biometrie (Muster in Zellstruktur, Blutgefäßen, Haut, Iris, …)	Sitzbelegung (grobe Kamera, Waage)	Gesichtsbild, Fingerabdruck, Handvenenmuster, Irisscan	– (nur mit zweitem Faktor möglich)
	1D-Code (Barcode)	EAN/GTIN, GS1[7]-Databar	(GS1-Databar innerhalb einer geschlossenen Domäne)	–
	PUF (Physical Unclonable Function)	z. B. Folien mit Ablösungskontrolle	Extraktion eines optischen Fingerabdrucks aus der Oberflächenbeschaffenheit	elektronische PUF im Mikroprozessor
	Beispiele gängiger Techniken/Methoden	Herkunftsnachweis, EAN[8]-Barcode, Bildmarke, „Made in Germany“	Platzkarte im Kino, Seriennummer, Visitenkarte, Fahrgestellnummer	elektronischer Personalausweis, Gesundheitskarte, Geldschein
	Beispiel aus der industriellen Produktion	Teilenummer (Typnummer) auf Maschinenteil … referenziert auf IEC 62433	Lizenzschlüssel bei Softwareinstallation … referenziert auf IEC 62433	Smart Meter … mit Industrie 4.0

1 Erläuterungen für den hellgrau unterlegten Bereich der Tabelle
X = ist mit diesem Typ von Identität möglich; (X) = ist mit diesem Typ von Identität eingeschränkt möglich; – = ist mit diesem Typ von Identität nicht möglich

2 Durch die Kombination einer eindeutigen Identität mit zusätzlichen Mechanismen zur Beweisführung kann eine Sichere Identität (SID) entstehen; deshalb ist die eindeutige Identität ohne Zusatzmaßnahmen nicht authentifizierbar

3 Media Access Control – die Hardwareadresse eines Netzwerkadapters, häufig bezogen auf Ethernet nach IEEE802.3

4 Trusted Platform Module, alternativ SW-, HW-Umsetzung

5 Radio Frequency Identification, gemeint ist ein System zur kontaktlosen Kommunikation zwischen einem elektronischen Lesegerät und einem (Sicherheits)Chip, der auf einem Objekt angebracht ist

6 Global Trade Item Number bzw. SGTIN = Serialized Global Trade Item Number

7 Global Standards One, Vergeber von GTINs als issuing agency nach ISO/IEC 15459-2

8 European Article Number, seit 2009 abgelöst durch GTIN

9 PUF (Physical Unclonable Functions): ein Funktionsmodul, welches eine auf seinen individuellen physikalischen Eigenschaften basierende eindeutige Identität bereitstellt, deren Echtheit beweist und im Rahmen gegebener Sicherheitsanforderungen nicht nachgebildet werden kann

tet auf bestimmte Ressourcen zugegriffen werden kann oder eine Identität komplett von weiteren Aktivitäten ausgeschlossen werden muss. Dies betrifft im Wesentlichen Authentisierungsvorgänge.

Auf jeden Fall muss man sich darauf einstellen, dass sich die Identität von Entitäten im Laufe der Zeit verändern kann und dass ggf. auch die zum Einsatz kommende Technik verändert werden muss, weil möglicherweise kryptographische Verfahren ihre Eignung verlieren.

Bei der Kommunikation in den Wertschöpfungsnetzwerken von Industrie 4.0 wird die unternehmensübergreifende Nutzung von Identitäten zunehmen. Das erfordert Vertrauen in die Ausgabestelle und den Kommunikationspartner.

Lebenszyklus einer Identität (Identitätsmanagement)

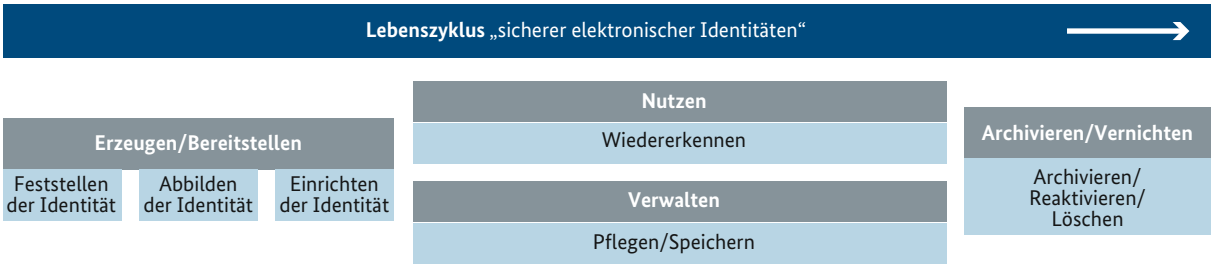
Um die Verwendung von Identitäten zu verstehen, soll hier der Lebenszyklus einer solchen kurz beschrieben werden. Es kann zwischen vier Phasen unterschieden werden. Die unterschiedlichen Rollen des Herstellers von Komponenten, des Maschinenbauers bzw. Integrators und des Betreibers von Anlagen sind zu berücksichtigen.

Mit der **Erzeugung der Identität** werden Identitätsattribute einer Entität erfasst und der Identität zugeordnet. Für eine sichere Identität erfolgt z. B. die Erzeugung eines digitalen Zertifikats und einer Signatur durch die ausgebende Stelle. Ein anderes Beispiel ist die Generierung eines Barcodes auf der Basis einer Seriennummer mit den notwendigen Informationen. Der Hersteller einer Komponente schafft damit die initiale Voraussetzung für die Verwendung. In der Rolle eines Maschinenbauers bzw. Integrators findet eine Aggregation der mit einer Identität versehenen Komponenten zu einer Maschine statt. Die erzeugte Identität bezieht sich in dieser Rolle auf die Maschine als Produkt, z. B. ein digitales Zertifikat als sichere Identität der Maschine oder eine Seriennummer für die Maschine. In der Rolle des Betreibers ist die erzeugte Identität, z. B. ein digitales Zertifikat, als sichere Identität der Maschine im Kontext des Unternehmens oder als Inventarnummer zu sehen. Auch eine Identifizierung entsprechend der Aufgabe der Maschine oder ihrem Standplatz[4] ist denkbar.

Die **Nutzung und Verwaltung** geschehen gleichzeitig. Bei der Nutzung wird die Identität zum Einsatz gebracht, beispielsweise authentisiert sich eine Maschine auf der Basis der sicheren Identität gegenüber einer anderen Maschine. Unter Verwaltung ist die Pflege, d. h. Aktualisierungen oder Ergänzungen von Identitätsattributen, deren Speicherung in zentralen oder dezentralen Systemen oder Anpassungen an den Berechtigungen einer Identität, zu verstehen. Im Rahmen der Nutzung anfallende Informationen bei der Verwendung der Identität können z. B. zum Tracing eingesetzt werden, um den aktuellen Standort einer Komponente zu ermitteln.

Den **Abschluss bilden die Archivierung** und Löschung einer Identität. Bei einer Archivierung werden bestimmte Inhalte weiterhin vorgehalten, um beispielsweise auf Parameter, die während der Produktion angefallen sind, weiter zurückgreifen zu können. Unter diesen Punkt fällt auch die Sperrung einer Identität, wenn beispielsweise ein Token entwendet wurde oder verlorengegangen ist. Die Folge ist, dass diese nicht weiter genutzt werden kann und eine neue sichere Identität erzeugt werden muss. Dabei kann auch auf die bestehenden Informationen zurückgegriffen werden.

Abbildung 3: Lebenszyklus einer sicheren Identität (angelehnt an ISO 29115)



Quelle: Plattform Industrie 4.0

4 Im Bereich von IT-Infrastrukturen ist dies üblich und wird z. B. über das SysLocation SNMP-Objekt abgebildet.

Die Nutzungsphase einer Identität ist in vielen Fällen zeitlich begrenzt. Physikalische Eigenschaften unterliegen der Alterung. Die Robustheit von kryptografischen Methoden kann durch allgemeinen technischen Fortschritt verringert werden (z. B. durch die steigende Verfügbarkeit von Rechenkapazität für sog. Brute-Force-Attacken). Solche Aspekte müssen insbesondere bei industriellen Anwendungsszenarien mit hoher Lebensdauer berücksichtigt werden, falls eine Überprüfung der Identität einer Komponente über den gesamten Lebenszyklus einer Anlage erforderlich ist.

Eine Identität spiegelt die Einordnung einer Entität in ihre Umgebung wider. Insofern kann eine Entität mehrere Identitäten gleichzeitig oder nacheinander haben, die der jeweiligen Rolle der Entität entsprechen. Für jede dieser Identitäten wird wiederum der Lebenszyklus Erzeugung/Nutzung und Verwaltung/Archivierung und Löschung durchlaufen, es wird also ein Identitätsmanagement benötigt.

Am Beispiel der oben genannten Maschine und der Rollen wird die besondere Herausforderung für sichere Identitäten deutlich: Bei der Inbetriebnahme der Maschine beim Betreiber wird z. B. eine sichere Identität in Form eines Zertifikats erzeugt und ist zu pflegen, sobald sich der Einsatzzweck verändert. Wird diese Maschine außer Betrieb genommen, ist darauf zu achten, dass die sichere Identität, die die Maschine als Maschine beim Betreiber ausweist, entsprechend behandelt wird, z. B. gelöscht wird.

Sichere Identitäten und Systemintegrität

Neben den sicheren Identitäten einer Entität muss sichergestellt werden, dass die bereitgestellten Funktionen wirklich die Funktionen sind, die vom Nutzer von der Entität erwartet werden. Es muss zum Beispiel ausgeschlossen werden, dass Entitäten Viren oder Trojaner enthalten, die die Integrität der Funktion einer Entität verletzen. Der Schutz der Identität allein ist deshalb eine notwendige, aber nicht hinreichende Maßnahme, um Sicherheit zu gewährleisten.

Der Erhalt der Integrität umfasst alle Wertschöpfungsketten von der Entwicklung, Produktion bis zum Betrieb der Entität. Damit ist ihr Erhalt eine Frage der entsprechenden Prozesse und auch der Maßnahmen, die zum Erhalt der Sicherheit in den Prozessen von allen Akteuren der Wertschöpfungskette betrieben werden.

Integrität ist keine statische Eigenschaft, sondern kann sich über die Lebensdauer der Entität verändern. Veränderung der Integrität kann beispielsweise durch Sicherheitslücken mit entsprechenden Angriffen entstehen, die zum Lieferzeitpunkt des Geräts unbekannt waren. Für den Betreiber einer Automatisierungsanlage stellt sich damit die Frage nach der Prüfung und dem Erhalt des Integritätsstatus seiner Automatisierungsanlage. Ferner müssen entsprechende Maßnahmen mit der Priorität der Verfügbarkeit der Anlage in Einklang gebracht werden.

4. Anforderungen an Identitäten in Industrie 4.0

Im Abgleich mit dem Stand der Dinge

Die IEC 62443, eine internationale Normreihe zur IT-Sicherheit industrieller Automatisierungssysteme (IACS), definiert vier Security-Level (SL1…SL4) auf der Basis technischer Security-Fähigkeiten. Der Security-Level orientiert sich an der Angriffsstärke, Level 1 berücksichtigt auch unbeabsichtigte Fehlbedienungen. Je höher der Security-Level, desto höher das erreichbare Sicherheitsniveau, siehe Tabelle 2 im Anhang A2.

Die benötigte Art der Identität ergibt sich aus der Bewertung der Beziehung zwischen den Entitäten und der damit geforderten Identifikation und Authentifizierung. Zur Authentifizierung wird ein Authentifizierer benötigt (z.B. Benutzername als Identifikation und Passwort zur Authentifizierung).

Die ISO/IEC JTC 1/SC 27 entwickelt Standards für den Schutz von Information und Kommunikation, mit Blick auf Sicherheit und Datenschutz. Dazu gehören u.a. kryptographische Mechanismen und Sicherheitsaspekte von Biometrie, Datenschutz und Identitätsmanagement. Zum Thema Identitätsmanagement gibt es folgende Aktivitäten:

- Identity management framework (ISO/IEC 24760); Teile 1 und 2 sind verabschiedet („Terminologie und Konzepte“, „Referenzarchitektur und Requirements“), der Teil 3 („Praxis“) ist gerade in Arbeit.
- Entity authentication assurance framework (ISO/IEC 29115, verabschiedet), High-level- und Technologie-agnostischer Überblick über grundsätzliche Aspekte von Authentication. Beinhaltet die Definition von vier Zuverlässigkeitsstufen von Authentisierung sowie Bedrohungen und Gegenmaßnahmen während des Authentisierungsprozesses.
- Authentisierung unter erhöhten Datenschutz-Anforderungen: Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, verabschiedet); Attribut-basierte Credentials (Studie)
- Access management framework (ISO/IEC 29146, in Arbeit), identity proofing (ISO/IEC 29003, in Arbeit)

ISO/IEC 24760, ISO/IEC 29115, ISO/IEC 29146 und ISO/IEC 29003 beziehen sich ausdrücklich auf die Authentisierung von Entitäten, die Personen oder Non-Person Entities (NPEs) sein können. Die Aktivitäten mit Datenschutz-Bezug beziehen sich dagegen meist auf die Identität von Personen oder Gruppen von Personen, nicht von Dingen.

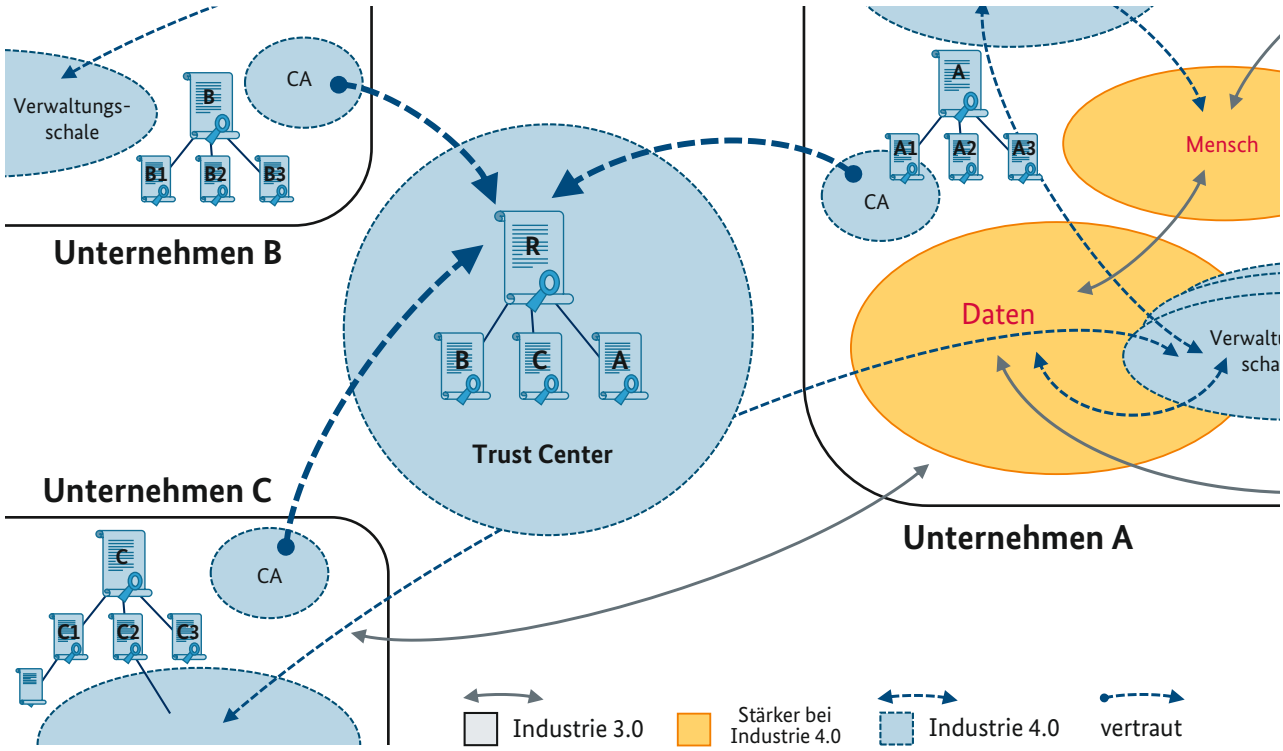
ISO 29115 Information technology -- Security techniques -- Entity authentication assurance framework: Diese Norm beschreibt ein Framework zur Verwaltung von Identitäten. Dabei werden verschiedene Stufen bzgl. der Zusicherung der Authentizität von Identitäten definiert und entsprechende Anforderungen definiert. Das Dokument kann Hinweise bei der Festlegung von Anforderungen geben.

Anforderungen für die Umsetzung sicherer Identitäten

Sicherheitsanforderungen ergeben sich aus den Schutzzielen und der Bedrohungsanalyse für den Anwendungsfall (bzw. auch allgemeiner für einen Anwendungsbereich).

Typische Schutzziele, die sich über die Anforderungen einer sicheren Authentifikation auf das erforderliche Sicherheitsniveau der Identitäten auswirken, sind:

Abbildung 4: Vertrauenswürdige „neutrale“ Instanz (Trust Center)



Quelle: Plattform Industrie 4.0

- Know-how-Schutz für Hersteller, Anlagenbauer und Betreiber
- Integrität der Produkt-/Systemfunktionen
- Vertraulichkeit von (kommunizierten) Daten
- Absicherung von Safety-Mechanismen (gegen beabsichtigte Störungen)

Das notwendige Sicherheitsniveau der Identität (u. a. mit PKI-Unterstützung, mit Hardware-Maßnahmen) ergibt sich aus der Risikobewertung unter Berücksichtigung der entstehenden Kosten.

Identitäten werden bislang innerhalb einer Sicherheitsdomäne (innerhalb eines Unternehmens) vergeben. Mechanismen und Regeln sorgen dafür, dass nur authentifizierte Entitäten an der Kommunikation teilnehmen.

Gefordert wird eine **vertrauenswürdige Stelle** (Certification Authority, CA) als Verwaltungsinstanz der Identitäten aller Entitäten in einer Sicherheitsdomäne. Aus heutiger Sicht erscheint eine PKI als mögliche Lösung, daher wird im Folgenden der Begriff Zertifizierungsstelle verwendet; siehe dazu auch Abbildung 2: Kommunikations- und Vertrauensbeziehungen bei Industrie 4.0.

Gängige Praxis im Office-Bereich ist heute eine zeitliche Befristung von Identitäten. Diese Vorgehensweise (zeitliche Befristung) ist zur Gewährleistung des Schutzziels Verfügbarkeit in der Produktion und im Produkt auf den Prüfstand zu stellen. Abhängig vom Anwendungsfall kann die Laufzeit der Identität an den Lebenszyklus gebunden sein bzw. durch den Verwender zeitlich bestimmt werden.

Die Nutzung der Vorteile der Industrie 4.0 erfordert sichere Wertschöpfungsnetzwerke und damit wird als erforderliches und essentielles Merkmal einer Entität in einem firmenübergreifenden Industrie 4.0-Wertschöpfungsnetzwerk eine sichere Identität gefordert, die über Sicherheitsdomänen hinweg nutzbar sein soll.

Die Abbildung illustriert eine zentrale Zertifizierungsstelle (Trust Center) als vertrauenswürdige Instanz in der Mitte der Abbildung für die Subskription von Zertifikaten in Sicherheitsdomänen.

Die Verifizierbarkeit der Identität über verschiedene Sicherheitsdomänen muss möglich sein. Vergabe und Entzug von Rechten muss unter Kontrolle der jeweiligen Domäne erfolgen.

Gefordert werden **Standards/Prozesse zur vertrauenswürdigen Kopplung der Zertifizierungstellen (CAs)** der jeweiligen Sicherheitsdomänen. Dazu gibt es bisher keine passende Vorlage. Konzept und Umsetzung könnten in Anlehnung an das Identitätsmanagement und die Roamingverträge der Mobilfunkprovider entstehen. Unternehmen (Sicherheitsdomänen) müssen anderen Unternehmen (anderen Sicherheitsdomänen) vertrauen.

Um ein belegtes Vertrauensniveau organisationsübergreifend zu verwenden, sind **Richtlinien und Prüfungsvorgaben in einen übergreifenden Security-Kontext für alle beteiligten Unternehmen** aufzunehmen.

Identitätsmanagement muss durchgängig den Schutz des geistigen Eigentums unterstützen. Dazu gehört u. a. die Limitierung der herstellbaren Produkte auf der Basis der bereitgestellten Produkt- und Produktionsmodelle. Ein akzeptiertes und anwendbares digitales Rechtemanagement ist eine wichtige Voraussetzung dafür.

Anforderungen an sichere Identitäten in der Produktentstehungsphase (Security-by-Design)

Die Sicherheit der Identitätsinformation spielt auch im Rahmen des „Security-by-Design“ eine wichtige Rolle. Das Ziel von „Security-by-Design“ ist es, Security-Funktionen als integrierten Teil eines Produkts bzw. einer Lösung zu realisieren. Neben einer klaren Verankerung von Security in den betroffenen Standards, und zwar von Anfang an, ergeben sich Konsequenzen für Hersteller und Betreiber von Anlagen. So sind umfassende Ergänzungen zu den bestehenden Prozessen erforderlich, die auch die Anforderungen an die Sicherheit der Identitäten und die Auswahl der Lösungsoptionen betreffen.

Im Rahmen von Security-by-Design werden an den „Security-Anker“ des Systems weitere Sicherheitsfeatures angeknüpft. Dabei werden in der Folge insbesondere die Sicherheitsniveaus von Funktionen für Vertraulichkeit und Integrität vom Niveau des Security-Ankers bestimmt.

Neben der Implementierung einer sicheren Identität in der physikalischen Produktion muss im Rahmen von Industrie 4.0 auch die entsprechende digitale/virtuelle Präsentation (**Verwaltungsschale**)[5] gesichert werden.

Im Rahmen des Security-by-Design müssen insbesondere auch Aspekte der Integration der „sicheren Identität“ in die Zielarchitektur berücksichtigt werden: Um sichere Identitäten nutzen zu können, sind oft auch Infrastrukturen für Schlüssel und deren Zertifikate erforderlich. Diese Infrastrukturen müssen im Design berücksichtigt und bereitgestellt werden. Insbesondere gilt hier auch die Regel, dass das Gesamtsicherheitsniveau einer Systemkette nicht größer sein kann als die Sicherheit des schwächsten Gliedes dieser Kette.

Security-by-Design betrifft auch das Thema Vertrauenswürdigkeit der Implementierung und der Prozesse: Es muss gewährleistet sein, dass die Sicherheit einer Identität nicht durch Schwächen in der Implementierung bzw. in den unterstützenden Prozessen kompromittiert werden kann: Die von einem Sicherheitsanker abhängigen Systemgeheimnisse dürfen nicht durch Seitenkanäle oder BackDoors unberechtigt ausgelesen werden können.

5 http://www.zvei.org/Downloads/Automation/Industrie%204.0_Komponente_Download.pdf

5. Handlungsempfehlungen

Die Umsetzung eines Identitäten-Konzepts wird immer Aufgabe der Unternehmen sein. Sie kennen ihre Prozesse und Notwendigkeiten am besten. Die Verantwortung der Politik ist es jedoch, gemeinsam mit der Industrie die Rahmenbedingungen für eine zielgerichtete, interoperable und effiziente sowie flächendeckende Infrastruktur zu schaffen. Insbesondere die Rollenverteilung zwischen staatlichen, PPP- und privatwirtschaftlichen Modellen ist gemeinsam zu diskutieren.

Die VDI/VDE-Richtlinie 2182 „IT-Security in der industriellen Automatisierung" beschreibt ein allgemeines Vorgehensmodell mit mehreren Prozessschritten. Berücksichtigt und verzahnt werden die Rollen des Herstellers von Komponenten, des Maschinenbauers bzw. Integrators und des Betreibers von Anlagen. Dem Betreiber der Anlage(n) kommt dabei die **Schlüsselrolle bezüglich Risikoanalyse** mit Identifikation und Bewertung der Gefährdungen hinsichtlich der IT-Security zu. Er legt die notwendigen Maßnahmen zur Risikoreduzierung und die sich daraus ergebenden Anforderungen an den Maschinenbauer/Integrator fest. **Analyse und Bewertung** müssen **regelmäßig** wiederholt werden. Der Maschinenbauer/Integrator ist aufgefordert, die aus der Betreibersicht erforderlichen Anforderungen entsprechend umzusetzen. Die notwendigen Voraussetzungen zur Umsetzung werden als Anforderungen an die Hersteller von Komponenten weitergegeben.

Abgeleitet aus diesem Vorgehensmodell ergeben sich für die Rollen (Hersteller, Maschinenbauer/Integrator, Betreiber von Anlagen, u. a. auch KMU) sowie für die Rolle der Politik differenzierte Handlungsempfehlungen.

Unternehmen als Betreiber

Der Betreiber von Anlagen ist aufgefordert, ein Sicherheitskonzept für seine Domäne zu entwickeln, zu verwalten und regelmäßig zu aktualisieren. Für die Wertschöpfungsketten und -netzwerke ist ein **Identitäten-Konzept aus Betreibersicht** zu erstellen, das notwendige Sicherheitsniveau der Identitäten ist zu ermitteln. Die sich daraus ergebenden Anforderungen sind an die Lieferanten der Maschinen und Anlagen weiterzugegeben.

Die Infrastruktur des Betreibers muss den Anforderungen aus dem Identitäten-Konzept gerecht werden, z. B. Aufbau einer vertrauenswürdigen Zertifizierungsstelle (Certification Authorities, CA) als Verwaltungsinstanz in einer Sicherheitsdomäne zur Verteilung und Verwaltung der sicheren Identitäten für alle Entitäten in der Produktionsebene (OT) unter Einbeziehung der Konzepte aus dem Office-Bereich (IT).

Maschinenbauer/Integrator

Aus Sicht des Maschinenbauers und auf der Basis der von ihm priorisierten Schutzziele ist ein **Identitäten-Konzept für die Maschine** zu entwickeln. Wo sind z. B. aufgrund des gewünschten eigenen Know-hows-Schutzes sichere

Identitäten innerhalb der Maschine notwendig? Die Identitäten der integrierten Komponenten sind auf der Basis des Konzepts zu prüfen. Die Identität, die der Maschine zugewiesen wird, soll an die Identitäten der integrierten Komponenten gebunden sein. Abgeleitet daraus ergeben sich die Anforderungen an die verbauten Komponenten und damit an den Hersteller der Komponenten.

Ferner sind die Anforderungen des Betreibers bezüglich des geforderten Sicherheitsniveaus der Identitäten zu berücksichtigen, z. B. die HW-Unterstützung zur sicheren Verwaltung einer Identität.

Die Infrastruktur des Maschinenbauers muss den Anforderungen aus dem Identitäten-Konzept für die Maschine gerecht werden, z. B. Aufbau einer vertrauenswürdigen Zertifizierungsstelle (Certification Authorities, CA) als Verwaltungsinstanz zum Einbringen von Schlüsselmaterial in die hergestellte Maschine bzw. in die verbauten Komponenten.

Im Kontext der Herstellung einer Maschine sind die Handlungsempfehlungen für einen Unternehmen als Betreiber mit zu berücksichtigen (Lieferantenanforderungen).

Komponentenhersteller

Hersteller sollten ihre Komponente mit einer angemessenen Identität versehen. Das Niveau (ID, UID oder SID) und die Stärke ihres Schutzes richten sich nach der möglichen Nutzung der Komponente im System. Die Maschinenbauer/Integratoren sollen in der Lage sein, die Echtheit der Komponente zu prüfen, wenn sie diese in ein System einbauen. Daher soll der Hersteller der Komponente eine angemessene Methode anbieten, mit der ein Maschinenbauer/Integrator diese Prüfung vornehmen kann.

Im Kontext der Herstellung eines Produkts sind die Handlungsempfehlungen für ein Unternehmen als Betreiber mit zu berücksichtigen.

Politik

Die Politik setzt durch Gesetze und Verordnungen den rechtlichen Rahmen, in dem die Akteure wie Betreiber, Integratoren und Komponentenhersteller handeln. Die für Industrie 4.0 erforderlichen Identitätskonzepte müssen im rechtlichen Rahmen umsetzbar sein. Dafür soll die Politik diese Konzepte bei Gesetzgebungsverfahren beachten. Relevante Bereiche sind u. a. Datenschutz und Vertragsrecht. Nationale Regelungen sollten in einem internationalen Kontext gesehen werden.

Eine hohe Vertrauenswürdigkeit technischer Lösungen kann zu einer Marke für Deutschland und Europa werden. Schon heute haben viele hochspezialisierte Anbieter von Lösungen für Cybersicherheit ihren Sitz in Deutschland. Der Aufbau vertrauenswürdiger IT-Infrastrukturen als Beitrag zur digitalen Souveränität Europas muss konsequent vorangetrieben werden. Dies muss jedoch durch entsprechende politische Initiativen unterstützt werden. Ziel ist es, die Security-Kompetenz und Vertrauenswürdigkeit deutscher und europäischer Unternehmen als entscheidenden Wettbewerbsfaktor zu stärken.

Offene Punkte:

Verfahren und Prozesse müssen beschrieben werden, die geeignet sind für ein automatisch verifizierbares Vertrauen zwischen Entitäten über Unternehmensgrenzen hinweg. Passende Vorlagen gibt es bislang nicht, denn die Herausforderung besteht darin, entsprechende Robustheit, Unabhängigkeit und technische Einheitlichkeit zu schaffen. Die Erfahrung beim Aufsetzen bisheriger Zertifizierungsstellen ist zu berücksichtigen, damit u. a. die Kompromittierung einzelner Zertifizierungsstellen nicht zum Problem von allen Entitäten wird.

Als Vorlage für ein neu zu erstellendes Konzept erscheinen die erfolgreichen Verfahren und Prozesse aus dem Identitätsmanagement und Roaming von Mobilfunkprovidern möglich.

Es stellt sich die Frage, ob für die unternehmensübergreifende Zusammenarbeit notwendige Prozesse und Produkte den von den Teilnehmern in der Wertschöpfungskette zu bestimmenden Sicherheitskriterien genügen müssen und entsprechend auditiert und klassifiziert werden sollten. Diese Einstufung könnte u. a. dem Einkauf des Betreibers bzw. Maschinenbauers eine deutliche Erleichterung bringen.

6. Anhang

A-1 Beispiele für Identitätskonzepte

Elektronische Bauelemente als Identitätsträger 1: RFID-Tag als Träger einer eindeutigen Identität (UID)

RFID-Tags sind Komponenten aus einer integrierten Schaltung (einem Mikrochip) und einer Antenne. Sie werden über das elektromagnetische Feld des Lesegeräts mit Energie versorgt. Der Abstand zwischen RFID-Tag und Lesegerät kann je nach Kommunikationsnorm bis zu 10 cm, bis zu 1 m oder mehrere Meter betragen. RFID-Tags speichern kleine Datenmengen (wenige hundert Byte) und haben begrenzte Sicherheitsfunktionen. Typischerweise tragen sie eine eindeutige Seriennummer (unique identifier, UID), die vom Chiphersteller während der Produktion in den Speicher geschrieben wurde. Die UID des Chipherstellers gilt im Kontext der Chipherstellung. Im Kontext der Nutzung des Chips kann sie auch als UID im Sinne von Tabelle 1 gelten, dies muss aber nicht automatisch der Fall sein. Die Zuordnung eines solchen RFID-Tags zum markierten Objekt geschieht durch die Zuordnung in der Verwaltungsschale. Die Daten im Speicher des RFID-Tags können nur gelesen werden, während er in der Reichweite eines Lesegeräts ist. Dies ist typischerweise nur während kurzer Zeiträume der Fall. Die Bauform hat einen Einfluss auf die Verwendung als Identitätsträger:

- **Ein aufgeklebter oder angeschraubter RFID-Tag** ist trennbar mit dem markierten Objekt verbunden. Er eignet sich als Träger von Identität (ID), für Logistikdaten und zur Beschleunigung und Vereinfachung von Inventurprozessen. Es muss im Einzelfall geprüft werden, ob ein solcher RFID-Tag noch mit dem Objekt verbunden ist, dem er ursprünglich zugeordnet wurde.

- **Ein fest eingeklebter RFID-Tag** ist untrennbar mit dem markierten Objekt verbunden. Bei der Lösung der Verklebung durch Hitze, chemische oder mechanische Einwirkung würde auch der RFID-Tag zerstört. Die Zuordnung zu einem bestimmten Objekt ist daher permanent und vertrauenswürdig. Dadurch eignet sich ein solcher RFID-Tag als Träger einer eindeutigen Identität (UID).

Elektronische Bauelemente als Identitätsträger 2: Sicherer Mikroprozessor

Sichere Mikroprozessoren können in Bauformen auftreten, die RFID-Tags ähnlich sehen. Manche Typen von sicheren Mikroprozessoren können wie diese durch das elektromagnetische Feld des Lesegeräts mit Energie versorgt werden; allerdings stets nur bei einer Reichweite von weniger als 10 cm. Im Gegensatz zu RFID-Tags sind sichere Mikroprozessoren komplexe Chips mit sehr umfangreichen Sicherheitsfunktionen. Sie haben ein eingebettetes Betriebssystem und eine Anwendungssoftware, die ihren Funktionsumfang bestimmt. Sie können Datenmengen bis zu mehreren hundert Kilobyte speichern. Sie berechnen komplexe kryptografische Algorithmen und können stark verschlüsselt kommunizieren. Ihr Speicherinhalt und alle Berechnungen sind verschlüsselt und gegen zahlreiche Arten von Angriffen gehärtet. Auch ihre Nutzung als Identitätsträger ist mit der Bauform verbunden:

- Ein **sicherer Mikroprozessor in einer Chipkarte** eignet sich als Träger einer Eindeutigen Identität (UID) für Menschen. Zwar ist eine solche Identität geschützt gegen die Erstellung von Kopien oder den unerlaubten Zugriff auf Daten auf der Karte. Die Zuordnung der Chipkarte zu ihrem rechtmäßigen Träger muss im System gegebenenfalls separat geprüft werden.

- Ein **aufgeklebter/angeschraubter sicherer Mikroprozessor** ist in seiner Verwendung ähnlich einem aufgeklebten/angeschraubten RFID-Tag und kann äußerlich gleich aussehen. Im Unterschied zu diesem erlaubt er aber das Speichern größerer Datenmengen, bietet einen erheblich stärkeren Schutz dieser Daten und eine verschlüsselte Kommunikation mit dem Lesegerät. Da er die Prüfung von Integrität, Fälschungsresistenz und Authentifikation ermöglicht, eignet er sich als Träger von Sicherer Identität (SID) im Kontext der Anwendung. Die trennbare Verbindung zum zugeordneten Objekt ist eine Beschränkung, die im System beachtet werden muss.

- Ein fest **in der Elektronik eines Geräts verbauter sicherer Mikroprozessor** benötigt im Gegensatz zu den vorgenannten Beispielen kein separates Lesegerät, da er mit der Elektronik des Geräts direkt verbunden ist. Er ermöglicht einen Onlinebetrieb der Sicherheitsprozesse im System. Neben der Bereitstellung einer Sicheren Identität (SID) mit starker Bindung an ein Gerät eignet sich ein solcher sicherer Mikroprozessor auch zur Authentifizierung, Verschlüsselung und Integritätsprüfung der Kommunikation im System. Bei der Nutzung eines solchen Mikroprozessors als Sicherheitsanker oder Identitätsträger muss beachtet werden, dass die umgebende Elektronik und die Übertragungswege im System

nicht automatisch sicher sind. Es kann eine Ende-zu-Ende-Verschlüsselung und Integritätsprüfung erforderlich sein, um Vertrauen auf der Systemebene sicherzustellen.

Vertrauensanker und sichere Identitäten

Für die Definition und Bewertung der Sicherheitsarchitektur eines Systems spielt der Begriff „Vertrauensanker“ (engl. „Trust Anchor“) eine wichtige Rolle:

Einerseits wird mit Vertrauensanker oft die Wurzelinstanz der Zertifikatshierarchie einer Public-Key-Infrastruktur bezeichnet.[6]

Andererseits wird mit Vertrauensanker einer Entität die Implementierung (=sichere Verankerung) der für diese Entität sensiblen Sicherheitsparameter (z. B. Integritätsprüfsummen und geheimes Schlüsselmaterial) bezeichnet.[7]

In jedem Fall hängt die Sicherheit des Gesamtsystems entscheidend vom Sicherheitsniveau der Vertrauensanker ab: Für Angreifer mehr oder weniger leicht zugängliche Softwareimplementierungen eines Vertrauensankers begründen offensichtlich ein geringeres Sicherheitsniveau als eine Einbettung der Sicherheitsparameter in abgeschottete Sicherheits-Hardware, die bei korrekter Integration mit Software-basierten Attacken von außen nicht kompromittiert werden kann.

Somit beruht auch das Sicherheitsniveau der Authentifikationsfunktion einer sicheren Identität letztlich auf der Qualität der im System und der Entität beteiligten Sicherheitsanker. Insbesondere für die Teilnahme an Industrie 4.0-Kommunikation über verschiedene Netzwerke hinweg werden sichere Identitäten mit entsprechenden Sicherheitsankern dringend benötigt. Ansonsten wird ein Partner im Kommunikationsverbund zu einem Sicherheitsrisiko, zum Beispiel weil die von ihm erzeugte Signatur fälschbar ist oder Schlüssel-Kryptoalgorithmen unberechtigt kopiert werden können.

Hardware-unterstützte Vertrauensanker können die Sicherheit IT-basierter Systeme deutlich verbessern. Allerdings genügt es nicht, Sicherheitsparameter und kryptographische Funktionen, die u. a. zur Authentifikation verwendet werden, innerhalb geschützter Hardware ablaufen zu lassen. Die Einbettung der Sicherheits-Hardware in das System muss im Rahmen von Security-by-Design entsprechend sicher gestaltet sein, um zusätzliche Angriffsstellen zu vermeiden.

Hardware-Komponenten, welche vorrangig zur Abwicklung von Sicherheitsfunktionen dienen, nennt man auch Sicherheitsmodule oder Secure Elements. Diese können Schlüssel sicher verwahren (zum Beispiel nicht kopierbar) und anwenden (zum Beispiel nicht belauschbar) und können außerdem den vertrauenswürdigen Zustand des Systems mittels Kryptografie gegenüber Kommunikationspartnern nachweisen (Remote Attestation).

Ein Beispiel für ein standardisiertes Sicherheitsmodul ist das sogenannte Trusted Platform Module (TPM) des Konsortiums „Trusted Computing Group“ (TCG). Ein TPM kann als spezieller Sicherheits-IC, als Funktionalität auf einem Standard-IC oder in Firmware realisiert sein. TPMs werden im Umfeld von Personal Computern, Mobilgeräten (Tablet, Smartphone) und Servern eingesetzt. Allerdings ist die Lebensdauer dieser Geräte auf deutlich weniger als 10 Jahre ausgelegt, was nicht zu den bekannten Lebenszyklen von Industriekomponenten passt. Im Rahmen des vom BMBF geförderten nationalen Referenzprojekts IUNO sollen Konzepte für Sicherheits-Hardware mit längeren Laufzeiten erforscht und bis 2018 gezielt in Demonstratoren zum Einsatz gebracht werden. Daneben gibt es vielerlei HW-basierte Sicherheitsmodule, die in IKT-Komponenten zum Einsatz kommen, in Bezahl-Terminals und Kreditkartensystemen, in Mobilfunksystemen, bei Mautsystemen, beim EU-Tachographen in der On-Bord-Unit in Lastkraftfahrzeugen oder auch bei den Kartenleseeinheiten beim Hausarzt.

6 http://tools.ietf.org/html/rfc5280, http://tools.ietf.org/html/rfc5914

7 http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5955006&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5955006,
http://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/trust-anchor-technologies-ds-45-734230.pdf

Vertrauenswürdige Instanz und deren Vernetzung; Mobilfunkstandards

Nach der Vorgabe durch den Standard sollte die International Mobile Station Equipment Identity (IMEI), eine 15-stelligen Seriennummer eines GSM- oder UTMS-Endgeräts, weltweit eindeutig sein. Die Sicherheit und Eindeutigkeit ist allerdings bei vielen Geräten nicht gewährleistet. Die SIM-Karte dient zur Identifikation des Nutzers. Zur eindeutigen Identifizierung des Netzteilnehmers dient die IMSI, die weltweit einmalig pro SIM von dem Mobilfunkprovider vergeben und auf der SIM-Karte gespeichert wird. Die Vergabe der IMSI erfolgt national (in D. durch die Bundesnetzagentur).

Die Authentizität des Mobilfunkteilnehmers gegenüber dem Provider wird sichergestellt, im Kontext Mobilfunk, unter dem Gesichtspunkt der korrekten Abrechnung durch den Provider.

Ein Mobilfunkprovider ist ein Beispiel für eine vertrauenswürdige Stelle (Certification Authoritiy, CA) als Verwaltungsinstanz der Identitäten aller Entitäten in einer Sicherheitsdomäne. Übertragen auf Industrie 4.0 repräsentieren SIM mit IMSI die Identität einer Industrie 4.0-Entität. Alle Entitäten, deren Identitäten durch eine solche CA vergeben werden, können unter Nutzung der CA die Authentizität der Identität des gewünschten Partners in einer Sicherheitsdomäne prüfen.

Roamingverträge der Mobilfunkprovider erlauben eine Kommunikation über Netzgrenzen hinweg. Übertragen auf Industrie 4.0 stellen Roamingverträge Verträge zwischen CAs dar und ermöglichen damit eine Kommunikations- und Vertrauensbeziehung über Sicherheitsdomänen hinweg.

A-2 Anforderungen an sichere Identitäten

Auf Basis der IEC 62443-3-3

Die IEC 62443, eine internationale Normreihe zur IT-Sicherheit industrieller Automatisierungssysteme (IACS), definiert vier Security-Level (SL1 ... SL4) auf der Basis technischer Security-Fähigkeiten. Der Security-Level orientiert sich an der Angriffsstärke, Level 1 berücksichtigt auch unbeabsichtigte Fehlbedienungen. Je höher der Security-Level, desto höher das erreichbare Sicherheitsniveau.

Tabelle 2: Anforderungen an sichere Identitäten auf Basis IEC 62443-3-3

	SL1	SL2	SL3	SL4
Identifizierung und Authentifizierung von menschlichen Nutzern	Anforderung ... alle menschlichen Nutzer zu identifizieren und zu authentifizieren. Diese Fähigkeit muss an allen Schnittstellen, die menschlichen Nutzern Zugang zum Automatisierungssystem gewähren, die Identifizierung und Authentifizierung durchsetzen ...	SL1 + Eindeutige Identifizierung und Authentifizierung	SL2 + Multifaktor-Authentifizierung über nicht vertrauenswürdige Netze	SL3 + Multifaktor-Authentifizierung über alle Netze
Identifizierung und Authentifizierung von Softwareprozessen und Geräten		Anforderung ... alle Softwareprozesse und Geräte zu identifizieren und zu authentifizieren. Diese Fähigkeit muss solche Identifikation und Authentisierung an allen Schnittstellen umsetzen, die Zugang zum Automatisierungssystem gewähren ...	SL2 + Eindeutige Identifizierung und Authentifizierung	SL2 + Eindeutige Identifizierung und Authentifizierung

→

Tabelle 2: Anforderungen an sichere Identitäten auf Basis IEC 62443-3-3 (Fortsetzung)

	SL1	SL2	SL3	SL4
Verwaltung der Authentifizierer	Fähigkeit … alle Authentifizierer vor einer nicht autorisierten Offenlegung und Änderung während der Speicherung und Übermittlung zu schützen	SL1	SL1 + Beglaubigung der Identität von Softwareprozessen durch Hardwaremaßnahmen	SL1 + Beglaubigung der Identität von Softwareprozessen durch Hardwaremaßnahmen
Passwortstärke	Fähigkeit … eine konfigurierbare Stärke von Passwörtern … durchzusetzen	SL1	SL1 + Erzeugung und Lebensdauerbeschränkungen von Passwörtern für menschliche Nutzer	SL3 + Lebensdauerbeschränkungen von Passwörtern für alle Nutzer
PKI-Zertifikate		Unterstützung PKI	SL2	SL2
Stärke der Authentifizierung durch öffentliche Schlüssel		… Prüfung öffentlicher und privater Schlüssel auf Gültigkeit …	SL2 + Schutz durch HW-Maßnahmen	SL2 + Schutz durch HW-Maßnahmen
Abgeleiteter Identitätstyp (vgl. Tabelle 1)	ID	SID	SID+	SID++

A-3 Begriffsdefinition Vertrauen

Vertrauen ist ein Konzept zur Modellierung der Überzeugung, dass eine Eigenschaft gültig ist, auch wenn die Gültigkeit im Einzelfall nicht beweisbar ist (insofern ein Glaube, der mittels Grundvertrauen aus Beobachtbarem ableitet und verallgemeinert). Für den speziellen Industrie 4.0-Kontext wäre es i. d. R. zu riskant, Vertrauen in dieser Form blind zu extrapolieren. Vertrauen ist hier feingranular und explizit durch die Überzeugung aufgrund erfolgreicher Überprüfung abzubilden, dass eine einzelne Security-Eigenschaft (z. B. Authentizität eines Absenders) zu einem spezifischen Zeitpunkt gültig ist. Dieses Vertrauen muss sowohl in Zeitpunkt als auch Qualität begründet sein durch die Kenntnis der Auswahl und des Einsatzes sowie von Qualitätsnachweisen über die technisch/organisatorischen Schutzmaßnahmen.

Da nicht alle Aspekte eines Security-Konzepts bei jeder einzelnen technischen Aktion jeweils geprüft werden können, muss weiterhin unterschieden werden zwischen allen relevanten umgebenden Security-Eigenschaften des Systems und der einzelnen naheliegenden/lokalen Security-Eigenschaft. Für beide Klassen ist eine explizite Vertrauensgrundlage nötig. Beispiele für Ersteres sind alle umgebenden Security-(System-) Eigenschaften, z. B. Security-Gesamtkonzept mit Arbeitsweise und Auswahl von Technologien und Gegenmaßnahmen unter Berücksichtigung von Standards, Best Practices, Zulassungen etc. Hier ist gesamtheitlich von Prozessebene bis Technik bei Design, Inbetriebnahme mittels einer Betriebsprüfung bzw. Audit oder Evaluation zu prüfen.

Die lokale Security-Eigenschaft ist die einzelne, innerhalb jeder Ausführung einer technischen Funktion/Aktion automatisiert überprüfbare Security-Eigenschaft. Diese Überprüfung erfolgt z. B. im Nachrichtenempfänger durch kryptografische Verifikation einer Signatur, die bei Erfolg die Integrität der Absenderadresse bestätigt und dadurch semantisch den Nachweis für die Authentizität der Nachricht erbringt.

Die Qualitätsnachweise bzw. die Prüfungen messen jeweils aktuelle Werte und vergleichen sie mit Sollwerten. Geforderte Sollwerte für „gut genug“ werden dabei von einer Security-Richtlinie definiert, welche auch den zeitlichen Aspekt (ab wann ist ein Nachweis „veraltet“?) berücksichtigt. Diese Grenzwerte für „gut genug“ und „veraltet“ werden dabei heute i. d. R. Unternehmens-spezifisch festgelegt. Damit ein belegtes Vertrauensniveau organisationsübergreifend wiederverwendet werden kann, ist die Aufnahme der Richtlinie und von Prüfungsvorgaben in einen übergreifend gültigen Security-Kontext notwendig.

Zurück im Beispiel bedeutet die Kombination von gesamtheitlicher und lokaler Prüfung, dass die eingesetzten Maßnahmen prinzipiell geeignet und qualitativ genügend gut umgesetzt sind, also der Richtlinie entsprechen (z. B. PKI-

-Signatur mit durchgängig immer in Hardware-Security-Modulen verwalteten privaten Schlüsseln). Es bedeutet weiterhin darauf aufbauend, dass für jede Nachricht der Empfänger mittels Signaturverifikation die Absendedaten kryptografisch auf Authentizität prüft. Durch eine Kopplung mit dem Nachrichteninhalt über eine Hashfunktion kann so die gesamte Nachricht hinsichtlich Authentizität und Integrität geprüft werden.

Diese lokale Prüfung vertraut dabei also implizit auf viele andere Security-Eigenschaften des Gesamtsystems, z. B. die Vertraulichkeit des privaten Schlüssels, also darauf, dass der private Schlüssel nur dem berechtigten Nutzer/Systemkomponente/Absender für die Signaturerstellung zur Verfügung steht. Automatisiert überprüfbar ist nur die lokale Eigenschaft durch kryptografische Signaturverifikation. Wenn aber mangels geeigneter Maßnahmen (z. B. fehlender 4-Augen-Zeremonie bei der Schlüsselerstellung) der private Schlüssel für die Signaturerstellung kompromittiert ist (z. B. Insider-Angriff), dann könnte der Angreifer unberechtigt formal korrekte Signaturen erstellen, die die lokale Signaturverifikation erfolgreich bestehen. Lokal ist die Kompromittierung nicht erkennbar, insofern benötigt die lokale Prüfung als Fundament das geprüfte Vertrauen in die umgebenden Security-Eigenschaften.

In dem beschriebenen mehrschichtigen Verfahren drückt das Vertrauen in die Security-Eigenschaft(en) auf Grundlage des Vertrauens in die umgebenden Security-Eigenschaften letztlich die begründete Erwartungshaltung aus, dass alle beim Security-Design berücksichtigten Angriffe auf die geschützten Security-Eigenschaften so aufwändig sind, dass ein vernünftiger, am Aufwand orientierter erfolgreicher Angriff unwahrscheinlich ist.

Bezüglich der PKI-Strukturen, die häufig zur Verwaltung von Identitäten genutzt werden, beschreibt die Technische Richtlinie BSI TR-03145 für Certification Authorities mit hohem Sicherheits-Level die für ein hinreichendes Vertrauen notwendigen angemessenen Maßnahmen (organisatorisch, technisch und bzgl. der Dokumentation).

A-4 Literaturverweise zu relevanten Standards und Normen

Über die genannten ISO-Standards

- Identity management framework (ISO/IEC 24760),
- Entity authentication assurance framework (ISO/IEC 29115)
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191)
- Access management framework (ISO/IEC 29146, in Arbeit)
- Identity proofing (ISO/IEC 29003, in Arbeit) gibt es weitere Publikationen, von denen hier einige genannt werden sollen. Eine sehr viel umfänglichere Zusammenstellung bietet das Dokument „Kompass der IT-Sicherheit[8]“ von DIN und Bitkom.

BSI TR-03126 sicherer RFID-Einsatz[9]

In verschiedenen Szenarien wird der Einsatz von RFID-Technologien betrachtet. Die Dokumente können als Leitfaden für Betreiber, Hersteller und Integratoren dienen, um eine sichere Umsetzung zu gewährleisten.

Privacy Impact Assessment Guideline for RFID Applications[10]

Es werden Betrachtungen bzgl. des Datenschutz-gerechten und sicheren Einsatzes von RFID gemacht. Die Dokumente können als Leitfaden für Betreiber, Hersteller und Integratoren dienen, um eine sichere Umsetzung zu gewährleisten.

8 https://www.bitkom.org/Publikationen/2014/Leitfaden/Kompass-IT-Sicherheitsstandards/140311-Kompass-der-IT-Sicherheitsstandards.pdf

9 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03126/index_htm.html

10 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile&v=1

DIN SPEC 16599 (Entwurf) Informationstechnik — Automatische Identifikation und Datenerfassungsverfahren – Rückverfolgbarkeit

Rückverfolgbarkeit hat einen hohen Stellenwert bei den strategischen Entscheidungen, die in die Produkt- und Prozessentwicklungen von Unternehmen einfließen. Die Empfehlung soll Möglichkeiten für die Realisierung von Rückverfolgungssystemen auf Basis vorhandener Standardmodule aufzeigen und so eine Lücke zwischen Technologie und Anwendung schließen. Sie beschreibt die eindeutige Kennzeichnung für Anwendungen der lokalen und der übergreifenden Rückverfolgbarkeit von Objekten (z. B. Rohmaterialien, Produkte, Container) über den gesamten Lebenszyklus.

DIN SPEC 16589 (Entwurf) Informationstechnik — Automatische Identifikation und Datenerfassungsverfahren – Rückverfolgbarkeit Produkt-zu-Internet-Kommunikation „Pointer to Process“

Die aus dem INS-Förderprojekt „Innovation mit Normen und Standards“ entwickelte DIN SPEC 16589 eröffnet eine vereinfachte Lösung der automatischen Verlinkung von einem Produkt oder Objekt mit dem Internet oder Intranet. Die mit „Pointer to Process (P2P)“ benannte Lösung verknüpft die unverwechselbare Identifikation, die für die Logistik benötigt wird, mit Prozessen, die über Netzwerke angestoßen werden, bzw. ablaufen. Dazu wird ein ISO-normierter Datenträger als optischer DATAMATRIX-Code oder RFID-Transponder verwendet, zum Beispiel ein elektronisches Typenschild nach DIN 66277. Die Objekt-ID des Typenschildes führt gleichzeitig zu einer Quelle über das Netz. Damit können automatische Prozesse nach dem Muster des „Internet der Dinge“ selbständig und ganz ohne externe Dienstleistung ausgelöst werden. Dies stellt eine Komponente zu Industrie 4.0 dar, da ein Objekt direkt über den Datenträger mit Steuerungssystemen kommunizieren kann. DIN SPEC 16589 „P2P“ ist damit ebenso für automatisierten Wartungs- und Störungsservice einsetzbar, bei dem der P2P-Objektcode über ein Smartphone die Verbindung zum Rechner aufbaut, in dem die Prozesse der Werkerführung, Information und Dokumentation ablaufen. Durch automatisch aufgebaute Kommunikation bei den automatischen oder manuellen Scanvorgängen sind punktgenaue Dokumentationen, Steuerungen und Rückverfolgungen von Vorgängen möglich.

AUTOREN DER AG SICHERHEIT VERNETZTER SYSTEME:

Dr. Lutz Jänicke, PHOENIX CONTACT Cyber Security AG | Michael Jochem (Leitung), Bosch Rexroth AG | Hartmut Kaiser, secunet Security Networks AG | Dr. Wolfgang Klasen, Siemens AG | Martin Klimke, Infineon Technologies AG | Dr. Bernd Kosch, Fujitsu Technology Solutions GmbH | Lukas Linke, ZVEI e.V. | Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik | Torsten Nitschke, PHOENIX CONTACT Software GmbH | Michael Sandner, Volkswagen AG | Mario Stoltz, NXP Semiconductors Germany GmbH | Thomas Walloschke, Fujitsu Technology Solutions GmbH | Steffen Zimmermann, VDMA e.V.

Diese Publikation ist ein Ergebnis der AG Sicherheit vernetzter Systeme (Plattform Industrie 4.0).

www.plattform-i40.de